Lecture 21
Brahmagupta-Pell Equation

Recall - For quadratic irrational x we defined

$$\begin{aligned}
x_0 = x &= \frac{B_0+\sqrt{d}}{C_0}, \quad C_0|d-B_0^2, \quad d, C_0, B_0 \in \mathbb{Z} \\
a_i &= \lfloor x_i \rfloor \\
x_i &= \frac{B_i+\sqrt{d}}{C_i} \\
x_{i+1} &= \frac{1}{x_i - a_i} \\
B_{i+1} &= a_i C_i - B_i \\
C_{i+1} &= \frac{d-B_{i+1}^2}{C_i}
\end{aligned}$$

We showed that $B_i, C_i \in \mathbb{Z}$, and that x has a purely periodic expansion if and only if $x > 1$ and $-1 < \overline{x} < 0$.

Corollary 72. *Let d be a positive integer, not a perfect square. Then the continued fraction of the number $x = \sqrt{d} + \lfloor \sqrt{d} \rfloor$ is purely periodic.*

Proof.

$$\begin{aligned}
&x = \sqrt{d} + \lfloor \sqrt{d} \rfloor > 1 \\
&\overline{x} = \sqrt{d} - \lfloor \sqrt{d} \rfloor \text{ satisfies } -1 < \overline{x} < 0 \text{ since } \lfloor \sqrt{d} \rfloor < \sqrt{d} < \lfloor \sqrt{d} \rfloor + 1
\end{aligned}$$

■

Let's analyze this $x = \sqrt{d} + \lfloor \sqrt{d} \rfloor$ a little more. $x = \frac{\sqrt{d}+\lfloor \sqrt{d} \rfloor}{1}$, and $1|d - \lfloor \sqrt{d} \rfloor^2$, so we can take $C_0 = 1$, and $B_0 = \sqrt{d}$. Want to see what happens for higher n - what x_n looks like. Let $x = [\overline{a_0, a_1, \ldots a_{r-1}}]$ be the continued fraction of x, r is chosen as smallest possible period.

Claim: $x_0 = x, x_1, x_2, \ldots x_{r-1}$ are all distinct

Proof. If $x_0 = x_i$ for some $i < r-1$, then we'd have period i smaller than r ■

So $x_n = x_o$ if and only if n is a multiple of r ($x_m = x_n$ if $m \equiv n \mod r$). We'll show that $C_n = 1$ if and only if n is a multiple of r, and C_n cannot be -1. First, if $n = kr$

$$\frac{B_{kr}+\sqrt{d}}{C_{kr}} = x_{kr} = x_n = x_0 = \sqrt{d} + \lfloor\sqrt{d}\rfloor$$

$B_{kr} - C_{kr}\lfloor\sqrt{d}\rfloor = \sqrt{d}(C_{kr}-1)$ only happens if $C_{kr} = 1$ (otherwise integer = irrational). Conversely, if $C_n = 1$ then $x_n = B_n + \sqrt{d}$.

We know x_n is also purely periodic $[\overline{a_n, a_{n+1}, \dots a_{n+r-1}}]$, so

$$\begin{aligned} & x_n > 1 \text{ and } -1 < \overline{x_n} < 0 \\ \Rightarrow & -1 < B_n - \sqrt{d} < 0 \\ \Rightarrow & B_n < \sqrt{d} < B_n + 1 \\ \Rightarrow & B_n = \lfloor\sqrt{d}\rfloor \end{aligned}$$

which means that $x_n = \sqrt{d} + \lfloor\sqrt{d}\rfloor = x_0$, so that n is a multiple of r.

Suppose $C_n = -1$. Then $x_n = -B_n - \sqrt{d}$ is purely periodic, so

$$x_n > 1 \Rightarrow -B_n - \sqrt{d} > 1$$

and

$$-1 < \overline{x_n} < 0 \Rightarrow -1 < -B_n + \sqrt{d} < 0$$

which means that $B_n > \sqrt{d}$ and $B_n < -\sqrt{d} - 1 \Rightarrow \sqrt{d} < -\sqrt{d} - 1$, which is impossible.

Note that $a_0 = \lfloor x\rfloor = \lfloor\sqrt{d} + \lfloor\sqrt{d}\rfloor\rfloor = \lfloor\sqrt{d}\rfloor + \lfloor\sqrt{d}\rfloor = 2\lfloor\sqrt{d}\rfloor$. So continued fraction expansion of $x = \sqrt{d} + \lfloor\sqrt{d}\rfloor$ is

$$[\overline{2\lfloor\sqrt{d}\rfloor, a_1, \dots a_{r-1}}] = [2\lfloor\sqrt{d}\rfloor, \overline{a_1, \dots a_{r-1}, 2\lfloor\sqrt{d}\rfloor}]$$

Continued fraction expansion of $\sqrt{d}$ will look like that of $\sqrt{d} + \lfloor\sqrt{d}\rfloor$ except with a different first digit $[\lfloor\sqrt{d}\rfloor, \overline{a_1, \dots a_{r-1}, 2\lfloor\sqrt{d}\rfloor}]$.

Note: We can run the (B_n, C_n) process for $x = \sqrt{d} = \frac{0+\sqrt{d}}{1}, C_0 = 1, B_0 = 0$, note that $x_1 = \frac{1}{x - \lfloor x\rfloor}$ is the same for $x = \sqrt{d}$ and for $x = \sqrt{d} + \lfloor\sqrt{d}\rfloor$, so since $x_n = \frac{B_n+\sqrt{d}}{C_n}$ is the same for these two x's as long as $n \geq 1$, and also because $x_n = \frac{B_n+\sqrt{d}}{C_n}$, then B_n, C_n are the same for $n \geq 1$ whether we start with $\sqrt{d}$ or $\sqrt{d} + \lfloor\sqrt{d}\rfloor$, so still true that $C_n \neq -1$ and $C_n = 1$ if and only if $n = kr$.

Theorem 73. *If $d \in \mathbb{N}$ is not a perfect square, and $\{\frac{p_n}{q_n}\}$ are the convergents to $\sqrt{d}$, and C_n is the sequence of integers we defined for x_n (starting with $x_0 = \frac{0+\sqrt{d}}{1}$), then $p_n^2 - dq_n^2 = (-1)^{n+1}C_{n+1}$.*

Proof.

$$\begin{aligned}\sqrt{d} = x_0 &= \frac{x_{n+1}p_n + p_{n-1}}{x_{n+1}q_n + q_{n-1}} \\ &= \frac{\left(\frac{B_{n+1}+\sqrt{d}}{C_{n+1}}\right)p_n + p_{n-1}}{\left(\frac{B_{n+1}+\sqrt{d}}{C_{n+1}}\right)q_n + q_{n-1}} \\ &= \frac{(B_{n+1}p_n + p_{n-1}C_{n+1}) + \sqrt{d}p_n}{(B_{n+1}q_n + q_{n-1}C_{n+1}) + \sqrt{d}q_n} \\ dq_n + \sqrt{d}(B_{n+1}q_n + q_{n-1}C_{n+1}) &= (B_{n+1}p_n + p_{n-1}C_{n+1}) + \sqrt{d}p_n\end{aligned}$$

By comparing coefficients, we get that

$$\begin{aligned}(B_{n+1}q_n + q_{n-1}C_{n+1})p_n &= p_n^2 \\ (B_{n+1}p_n + p_{n-1}C_{n+1})q_n &= dq_n^2 \\ C_{n-1}\underbrace{(p_n q_{n-1} - q_n p_{n-1})}_{(-1)^{n-1}} &= p_n^2 - dq_n^2 \\ p_n^2 - dq_n^2 &= (-1)^{n+1}C_{n+1}\end{aligned}$$

■

Corollary 74. *If r is period of the continued fraction expansion of $\sqrt{d}$, then $p_{kr-1}^2 - dq_{kr-1}^2 = (-1)^k r$.*

Remark 2. If nr is even then we get a solution (p_n, q_n) of the P-B equation since $p_{kr-1}^2 - dq_{kr-1}^2 = (-1)^{\text{even}} = 1$, so we get infinitely many solutions since convergents are all distinct.

Back to P-B equations $x^2 - dy^2 = 1$ with $d \in \mathbb{Z}$, want $x, y \in \mathbb{Z}$. If $d \leq 0$, then $x^2 + |d|y^2 = 1$, since $x, y \in \mathbb{Z}$, finite number of easily computed solutions. So, can assume $d > 0$. We showed last time that in fact, all solutions must come from continued fraction of $\sqrt{d}$.

More generally, (*) $x^2 - dy^2 = N$ for $N \in \mathbb{Z}$. If (x, y) is a solution of (*), then so is $(\pm x, \pm y)$ for any choice of signs. Some trivial solutions for $x = 0$ or $y = 0$, so look for nontrivial. Then we can assume $x, y > 0$. These are called positive solutions. Also assume that $(x, y) = 1$. (If not, replace N with $\frac{N}{g^2}$ if $g = (x, y)$). So only looking for positive, primitive (x, y).

Theorem 75. *Let $d \in \mathbb{N}$, $d \neq \square$, and let $N \in \mathbb{Z}$ such that $|N| < \sqrt{d}$. Then any positive primitive solution (x, y) of $x^2 - dy^2 = N$ has the property that $\frac{x}{y}$ is a convergent to $\sqrt{d}$.*

Proof. Suppose ρ is a positive real number such that $\sqrt{\rho}$ is irrational and $\sigma \in \mathbb{R}$,

$s, t \in \mathbb{N}$ such that $s^2 - t^2\rho = \sigma$ and also that $0 < \sigma < \sqrt{\rho}$.

Claim:

$$\left|\frac{s}{t} - \sqrt{\rho}\right| < \frac{1}{2t^2}$$

Proof of Claim.

$$\begin{aligned}\frac{s}{t} - \sqrt{\rho} &= \frac{s - t\sqrt{\rho}}{t} \\ &= \left(\frac{(s - t\sqrt{\rho})(s + t\sqrt{\rho})}{t(s + t\sqrt{\rho})}\right) \\ &= \frac{s^2 - t^2\rho}{t(s + t\sqrt{\rho})} \\ &= \frac{\sigma}{t(s + t\sqrt{\rho})}\end{aligned}$$

Note that because $s^2 - t^2\rho = \sigma > 0$, $s > t\sqrt{\rho}$, so $s + t\sqrt{\rho} > 2t\sqrt{\rho}$, so that

$$0 < \frac{s}{t} - \sqrt{\rho} < \frac{\sigma}{t - 2t\sqrt{\rho}} < \frac{\sqrt{\rho}}{2t^2\sqrt{\rho}} = \frac{1}{2t^2}$$

□

Now, using the claim we see that $\frac{s}{t}$ is a convergent to the continued fraction of $\sqrt{\rho}$ (by Problem 4 of PSet 9).

If $N > 0$, just use $\sigma = N, \rho = d, (s, t) = (x, y)$ to show that $\frac{x}{y}$ is a convergent to $\sqrt{d}$. If $N < 0$, rewrite $x^2 - dy^2 = N$ as $y^2 - \frac{1}{d}x^2 = -\frac{N}{d}$, then take $\sigma = -\frac{N}{d}$. $|N| < \sqrt{d}$, so $0 < \sigma < \frac{\sqrt{d}}{d} = \frac{1}{\sqrt{d}}$, and so $\frac{y}{x}$ is a convergent to continued fraction of $\frac{1}{\sqrt{d}}$.

Note that if the continued fraction of $\sqrt{d} = [a_0, a_1, \ldots]$, then continued fraction of $\frac{1}{\sqrt{d}} = [0, a_0, a_1, \ldots]$ means that convergents of $\frac{1}{\sqrt{d}}$ are just reciprocals of convergents of $\sqrt{d}$.

$$[0, a_0, a_1, \ldots] = \frac{1}{a_0 + \frac{1}{\ddots_{a_k}}} = \frac{1}{\frac{p_k}{q_k}} = \frac{q_k}{p_k}$$

and so if $\frac{y}{x}$ is a convergent to $\frac{1}{\sqrt{d}}$, then $\frac{x}{y}$ is a convergent to $\sqrt{d}$ ■

Theorem 76. *Let $d \in \mathbb{N}, d \neq \square$. All positive solutions to $x^2 - dy^2 = \pm 1$ are of the form $(x, y) = (p_n, q_n)$ where $\frac{p_n}{q_n}$ is convergent to $\sqrt{d}$. If r is the period of the continued fraction of $\sqrt{d}$, then*

- *If r is even, $x^2 - dy^2 = -1$ doesn't have any solutions, and all positive solutions of $x^2 - dy^2 = 1$ are given by $x = p_{kr-1}, y = q_{kr-1}$ for $k = 1, 2, 3, \ldots$.*

- *If r is odd, then all positive solutions to $x^2 - dy^2 = -1$ are given by taking $x = p_{kr-1}, y = q_{kr-1}$ for $k = 1, 3, 5, \ldots$, and all positive solutions to $x^2 - dy^2 = 1$ are given by taking $x = p_{kr-1}, y = q_{kr-1}$ for $k = 2, 4, 6, \ldots$*

Proof. If (x, y) is a positive solution to $x^2 - dy^2 = \pm 1$ then $\gcd(x, y) = 1$ is forced. By theorem it must come from convergent to $\sqrt{d}$, say $\frac{p_n}{q_n}$. But we showed that $p_n^2 - dq_n^2 = (-1)^{n+1}C_{n+1}$. Also C_{n+1} can't be -1, and can be 1 if and only if $n + 1$ is a multiple of r - ie., $n = kr - 1$. So, $p_{kr-1}^2 - dq_{kr-1}^2 = (-1)^{kr} \Rightarrow$ if r even, can't be -1, and if r odd, can be ± 1. ■

Remark 3. Suppose two positive solutions (x_1, y_1) and (x_2, y_2) are solutions of $x^2 - dy^2 = 1$, then $x_1 < x_2 \iff y_1 < y_2$.

Proof. $y_1 < y_2 \Rightarrow x_1^2 = 1 + dy_1^2 < 1 + dy_2^2 = x_2^2$ and $x_1, x_2 > 0$ so $x_1 < x_2$. Same for other direction, which means that we can order the positive solutions ■

Theorem 77. *If (x_1, y_1) is the least positive solution of $x^2 - dy^2 = 1$ where $\square \neq d \in \mathbb{N}$, then all positive solutions are given by (x_n, y_n) where $x_n + \sqrt{d}y_n = (x_1 + \sqrt{d}y_1)^n$.*

Eg. For $x^2 - 2y^2 = 1$, $(3, 2)$ is the smallest positive solution. Then $(3 + 2\sqrt{2})^2 = 17 + 12\sqrt{2} \Rightarrow (17, 12)$ is the next solution.

18.781 Theory of Numbers
Spring 2012